UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,815	01/30/2004	Frederick J. Murphy	1674.00001	5636

86636   7590   03/15/2011
BRUNDIDGE & STANGER, P.C.
2318 MILL ROAD, SUITE 1020
ALEXANDRIA, VA 22314

EXAMINER
CRIBBS, MALCOLM

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
03/15/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<table>
<tr><td rowspan="3">Office Action Summary</td><td colspan="2">Application No.
10/767,815</td><td colspan="2">Applicant(s)
MURPHY ET AL.</td></tr>
<tr><td colspan="2">Examiner</td><td>Art Unit</td><td></td></tr>
<tr><td colspan="2">/MALCOLM CRIBBS/</td><td>2432</td><td></td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2011*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17,19,22-24,27 and 28* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-17,19,22-24,27 and 28* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

This action is in response to the correspondence filed on 12/14/2010.

Claims 1-28 are presented for examination.

Response to Arguments

1.   Acknowledgement to Applicant's amendment to claims 1 and 13 is noted. The amendment has been reviewed, entered and overcomes the previously raised objection for minor informalities. Objections to claims 1 and 13 are hereby withdrawn.

2.   Acknowledgement to Applicant's amendment to claim 4 is noted. The amendment has been reviewed, entered and overcomes the previously raised objection for minor informalities. Objection to claim 4 are hereby withdrawn.

3.   Acknowledgement to Applicant's cancelling of claims 18, 20, 21, 25, and 26 is noted. The amendment has been reviewed, entered and overcomes the previously raised claim rejection under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Rejections to claims 18, 20, 21, 25, and 26 are hereby withdrawn.

4.   Applicant's arguments with respect to claims 1-17, 19, 22-24, 27, and 28 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claim 1 is objected to because of the following informalities: In claim 1, the Examiner suggest determining said regulatory compliance ... instead of *applying* as determining more clearly states the intentions of the present invention and coincides with the applicant's specification. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 1 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 recites subject matter which has the option of human operations only (*i.e. transforming into non-electronic forms; human completion of data screens; human conversion; and non-electronic feedback*) thus not necessitating machine implementation which is directed to non-statutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Publication Number 2003/0004734 to Alder et al. (hereinafter Alder) in view of Publication Number US 2003/0088520 to Bohrer et al. (hereinafter 'Bohrer') in view of Publication Number US 2005/0131839 to Cordery et al. (hereinafter 'Cordery').

As to claims 1 and 13, Alder teaches a method of secure privacy notification in accordance with regulatory compliance requirements, said method comprising the steps: applying the said regulatory compliance requirements for privacy notification of

data subjects (*paragraph [0041], [0042], [0086], [0088]*); and transforming said requirements into electronic database query screens and forms (*paragraph [0008], [0041], [0042]; wherein the forms of the invention including the privacy policy can be enforced either manually or via automation thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use electronic screens and forms for automation and non-electronic screens and forms for manual enforcement*); human or automated completion of said data screens (*paragraph [0008], [0041], [0042]; wherein the forms of the invention including the privacy policy can be enforced either manually or via automation thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use electronic screens and forms for automation and non-electronic screens and forms for manual enforcement*); human and/or automated conversion of data screens into privacy notification human readable formats (*paragraph [0008], [0042], [0043], [0088]*).

Alder does not explicitly teach querying a remote and/or resident database for information fields contained within said query screens and forms; electronic and/or non-electronic data subject feedback response methods and means; and conversion of said data subject's feedback responses into database deletion, modification or correction of the data subject's information in accordance with said regulatory requirements.

Bohrer teaches a method of enforcing privacy preferences on exchanges of personal data over a computer network (*Abstract*). Bohrer teaches querying a remote and/or resident database for information fields contained within said query screens and forms (*paragraph [0082], [0088]*); electronic and/or non-electronic data subject feedback

response methods and means (*paragraph [0036], [0082], [0088]; wherein the data subject's consent can be required in which an email is sent to the data subject in order to indicate in a response whether to deny or allow or input missing data for the request*); and conversion of said data subjects feedback responses into database deletion, modification or correction of the data subject's information in accordance with said regulatory requirements (*paragraphs [0033], [0035], [0082], [0088]; wherein the data subject is requested to give consent on allowing or denying access and to modify or correct missing information*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of enforcing privacy preferences as taught by Bohrer in the system of Alder in order to allow a data subject to express privacy preference policies for controlling access to their personal data and gives the data subject complete freedom to specify their own their own privacy preference policies for any data exchange request (*paragraph [0017]*).

Bohrer teaches a method of enforcing privacy preferences on exchanges of personal data across a network for business transactions such as e-Wallet (*paragraph [0001]-[0003]*). Neither Alder nor Bohrer explicitly teach encryption/decryption of said data screens.

Cordery teaches another method of facilitating transactions of business such as e-Wallet (FIG. 3 e-Wallet 10) by transmitting data trough a network between various parties (*Abstract; paragraphs [0001], [0048]*). Cordery teaches encryption/decryption of data screens (*paragraph [0046], [0064], and [0081]*).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the method of facilitating business transaction as taught by

Cordery in the modified system of Alder and Bohrer in order to provide secure data

communications transmitted through a network with confidential or private information

(*paragraph [0059], [0064]*).

Claims 2, 3, 22, and 23 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Alder in view of Bohrer in view of Cordery in further view of

Publication Number US 2003/0065727 to Clarke et al. (hereinafter 'Clarke').

As to claim 2, neither Alder, Bohrer, nor Cordery teach the electronic privacy

notification and feedback response is accomplished via a secure web portal.

Clarke teaches a method of providing secured messaging in a communications

network environment between customer locations for e-business transactions (*Abstract;*

paragraphs [0011], [0012]). Clarke teaches the electronic communication is

accomplished via a secure web portal (*paragraph [0057]*).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the method of communications via a network for business

transactions in the modified system of Alder, Bohrer, and Cordery in order to provide a

secure communication means in which to transmit private or confidential data

(*paragraphs [0012], [0029]*).

As to claims 3 and 23, neither Alder, Bohrer, nor Cordery teach the electronic

privacy notification and feedback response is accomplished via a secure e- mail system.

Clarke teaches a method of providing secured messaging in a communications

network environment between customer locations for e-business transactions (*Abstract;*

paragraphs [0011], [0012]). Clarke teaches the electronic privacy notification and

feedback response is accomplished via a secure e- mail system (*paragraphs [0013],*

[0016], and [0057]).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the method of communications via a network for business

transactions in the modified system of Alder, Bohrer, and Cordery in order to provide a

secure communication means in which to transmit private or confidential data

(*paragraphs [0012], [0029]*).

As to claim 22, neither Alder, Bohrer, nor Cordery teach the electronic privacy

notification and feedback response is accomplished via a secure socket layer web

portal.

Clarke teaches a method of providing secured messaging in a communications

network environment between customer locations for e-business transactions (*Abstract;*

paragraphs [0011], [0012]). Clarke teaches the electronic privacy notification and

feedback response is accomplished via a secure socket layer web portal (*paragraphs*

[0040], [0064]).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the method of communications via a network for business

transactions in the modified system of Alder, Bohrer, and Cordery in order to provide a

secure communication means in which to transmit private or confidential data

(*paragraphs [0012], [0029]*).

Claims 4, 5, and 28 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Alder in view of Bohrer in view of Cordery in further view of

Publication Number US 2003/0115468 to Aull et al. (hereinafter 'Aull').

As to claim 4, Bohrer teaches alerting the data processor of both the data

subject's privacy preferences and legal and regulatory compliance requirements

relevant to the data subjects privacy preferences (*paragraphs [0035], [0081], [0082],*

[0088]); and Cordery teaches the used of communication using digital certificates

(*paragraph [0052]*), however neither Bohrer, nor Cordery explicitly teach the electronic

privacy notification and feedback response is accomplished using digital certificates

comprising: a public or private, commercial or government registration authority; a

public or private, commercial or government certificate authority; a digital signature

encryption algorithm' a unique non-reputable user electronic identity; issuance of x.509

compliant certificates specifically encoded via extension to alert data processor of the

data subjects privacy preferences; and issuance of x.509 standard certificates

specifically encoded via extension to alert data processors of legal and regulatory

compliance requirements relevant to the data subjects privacy preferences.

Aull teaches a method facilitating secure communications through a network by

the use of digital certificates (*abstract; paragraphs [0002], [0017]*). Aull teaches a public

or private, commercial or government registration authority (*paragraphs [0028], [0031]*);

a public or private, commercial or government certificate authority (*paragraphs [0028],*

[0031]); a digital signature encryption algorithm (*paragraphs [0006], [0009]*); a unique

non-reputable user electronic identity (*table 1; paragraphs [0028], [0031]*); issuance of

x.509 compliant certificates specifically encoded via extension to alert data processor of

the data subjects privacy preferences (*paragraph [0026], [0028], [0031]*); and issuance

of x.509 standard certificates specifically encoded via extension to alert data processors

of legal and regulatory compliance requirements relevant to the data subjects privacy

preferences (*paragraph [0026], [0028], [0031]*).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the method of facilitating secure communications as taught

by Aull in the modified system of Alder, Bohrer, and Cordery in order to verify the

identity and credentials of the sender and to restrict access to only those whom are

authorized (having the correct key) to receive and view the communication (*paragraph

[0031]*).

As to claim 5, Aull teaches the digital signature algorithm is SHA-1 with DSA

(*paragraph [0006], [0009]*).

As to claim 28, Bohrer teaches the binding of a user's identity and access

authorizations to software tokens and challenging the tokens at a remote email server

or secure web portal in order to gain access to the users authorized email or web

messages (*paragraph [0046]*).

**Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over
Alder in view of Bohrer in view of Cordery in further view of Patent Number US
7,493,497 to Tan, Jr. (hereinafter 'Tan').**

As to claim 14, neither Alder, Bohrer, nor Cordery teach a USB key that containing encryption and processing circuitry, authorized user bound identity information and volatile and/or non-volatile memory that stores the algorithms used to query for said data fields.

Tan teaches another method of facilitating secure electronic communications through a network (*abstract; column 1, line 29-42*). Tan teaches a USB key that containing encryption and processing circuitry, authorized user bound identity information and volatile and/or non-volatile memory that stores the algorithms used to query for said data fields (*column 3, line 51-54; and column 3, line 62 to column 4, line 58*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of facilitating electronic communications as taught by Tan in the modified system of Alder, Bohrer, and Cordery in order to provide secure communications by validation and authentication of external systems to secure the privacy of electronic data exchange and transactions of the system (*column 1, line 29-42; and column 4, line 59 to column 5, line 3*).

Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in further view of Publication Number US 2004/0078599 to Nahum.

As to claim 15, neither Alder, Bohrer, nor Cordery teach a hardware firewall that contains encryption and processing circuitry, authorized user bound identity information

and volatile and/or non- volatile memory that stores the algorithms used to query said data fields.

Nahum teaches a method of securing data stored in a storage accessible over a network (*abstract; paragraph [0014]*). Nahum teaches a hardware firewall that contains encryption and processing circuitry, authorized user bound identity information and volatile and/or non- volatile memory that stores the algorithms used to query said data fields (*paragraph [0086]; wherein it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a firewall as software or hardware based on user desirability*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of securing data accessible over a network in the modified system of Alder, Bohrer, and Cordery in order to restrict access to the data by unauthorized users thus providing security by keeping the unauthorized user isolated from the storage (paragraph [0086]).

As to claim 16, neither Alder, Bohrer, nor Cordery teach a software firewall that contains encryption and processing instruction sets, authorized user bound identity information and volatile and/or non- volatile memory that stores the algorithms used to query said data fields.

Nahum teaches a method of securing data stored in a storage accessible over a network (*abstract; paragraph [0014]*). Nahum teaches a software firewall that contains encryption and processing instruction sets, authorized user bound identity information and volatile and/or non- volatile memory that stores the algorithms used to query said

data fields (*paragraph [0086]; wherein it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a firewall as software or hardware based on user desirability*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of securing data accessible over a network in the modified system of Bohrer, and Cordery in order to restrict access to the data by unauthorized users thus providing security by keeping the unauthorized user isolated from the storage (paragraph [0086]).

Claims 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder, Bohrer in view of Cordery in further view of Applicant's Admitted Prior Art (hereinafter 'AAPA').

As to claim 17, Bohrer teaches deriving privacy regulatory compliance requirements for the protection of personal data (*paragraphs [0005]-[0007]*), however neither Alder, Bohrer, nor Cordery teach the privacy regulatory compliance requirements are derived from the laws, rules and regulations promulgated by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

AAPA teaches a method of protecting personal data using privacy policies. AAPA teaches that the European Union Privacy Directive objective was to protect personal data, thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to derive privacy regulatory compliance requirements based on the European Union Privacy Directive to protect personal data (*Specification page 4, 2nd paragraph of the background of the invention*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of protecting personal data using privacy polices as taught by AAPA in the modified system of Alder, Bohrer, and Cordery in order to protect personal data from unintended or unknown access by unauthorized users (*Specification page 4, 2nd paragraph of the background of the invention*).

As to claim 19, Bohrer teaches deriving privacy regulatory compliance requirements for the protection of personal data (*paragraphs [0005]-[0007]*), however neither Alder, Bohrer, nor Cordery the privacy regulatory compliance requirements are derived from the laws, rules and regulations promulgated by The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

AAPA teaches a method of protecting personal data using privacy policies. AAPA teaches that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) objective was to protect the confidentiality and privacy of personal data, thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to derive privacy regulatory compliance requirements based on the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect personal data (*Specification page 4, 1st paragraph of the background of the invention*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of protecting personal data using privacy polices as taught by AAPA in the modified system of Alder, Bohrer, and Cordery in order to protect personal data from unintended or unknown access by unauthorized users (*Specification page 4, 1st paragraph of the background of the invention*).

Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in further view of Publication Number US 2005/0132188 to Khin et al. (hereinafter 'Khin').

As to claim 24, Bohrer teaches receiving feedback from data subjects via email (*paragraph [0036], [0082], [0088]*), however neither Alder, Bohrer, nor Cordery teach the privacy notification and feedback response is accomplished via postal notification.

Khin teaches a method of determining and implementing privacy requirements regarding personal information (*abstract; paragraph [0010]*). Khin teaches the privacy notification and feedback response is accomplished via postal notification (*paragraph [0039], [0070]*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of implementing privacy requirements in the modified system of Alder, Bohrer, and Cordery in order to provide the customer the ability to decide whether their data should be shared in a rare instance in which e-mail or the network is unavailable (*paragraph [0070]*).

Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Patent Number US 7,218,735 to Coron et al. (hereinafter 'Coron').

As to claim 6, neither Alder, Bohrer, Cordery, nor Aull teach the digital signature algorithm is an elliptic curve.

Coron teaches a method of generating digital signatures for secure

communication (abstract). Coron teaches the digital signature algorithm is an elliptic

curve (abstract; column 3, line 10-22).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the digital signature generation method as taught by Coron

in the modified system of Alder, Bohrer, Cordery, and Aull in order to further provide

secure communications while allowing the ability to validate the message originator

(abstract; column 3, line 10-22).

As to claim 7, Coron teaches the elliptic curve is a Koblitz binary curve (abstract;

column 3, line 10-22).

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alder

in view of Bohrer in view of Cordery in view of Aull in further view of Publication

Number US 2002/0150241 to Scheidt et al. (hereinafter 'Scheidt').

As to claim 8, neither Alder, Bohrer, Cordery, nor Aull teach the digital signature

algorithm is a block cipher such as Rijndael.

Scheidt teaches a method of electronically signing a document to communicated

over a network using a digital signature (abstract; paragraph [0011], [0012]). Scheidt

teaches the digital signature algorithm is a block cipher such as Rijndael (*paragraph*

[0084]).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the method of electronically signing a document using a

digital signature as taught by Scheidt in the modified system of Alder, Bohrer, Cordery,

and Aull in order to provide secure communications by providing resistance to counterfeiting of the written signature and the data/document itself being transmitted (paragraph [0011]).

Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Publication Number US 2004/0098285 to Breslin et al. (hereinafter 'Breslin').

As to claim 9, Bohrer teaches the data subject's privacy preference is to "opt out" (*paragraphs [0011], [0082]*). Neither Alder, Bohrer, Cordery, nor Aull teach where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

Breslin teaches a method of assessing, monitoring, and managing risk management of data privacy (*abstract*). Breslin teaches where encoding the digital certificate to be easily read by visual inspection by distinct color coding (*paragraph [0072]*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the risk management of privacy data method as taught by Breslin in the modified system of Alder, Bohrer, Cordery, and Aull in order to provide the user the ability to visually quickly determine the status of the digital certificate (*paragraph [0072]*).

As to claim 10, Bohrer teaches the data subject's privacy preference is to "opt in" (*paragraphs [0011], [0082]; wherein the data subject consents to allow*). Neither

Alder, Bohrer, Cordery, nor Aull teach where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

Breslin teaches a method of assessing, monitoring, and managing risk management of data privacy (*abstract*). Breslin teaches where encoding the digital certificate to be easily read by visual inspection by distinct color coding (*paragraph [0072]*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the risk management of privacy data method as taught by Breslin in the modified system of Alder, Bohrer, Cordery, and Aull in order to provide the user the ability to visually quickly determine the status of the digital certificate (*paragraph [0072]*).

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Publication Number US 2003/0035548 to Kwan.

As to claim 11, neither Alder, Bohrer, Cordery, nor Aull teach including third party archiving of certificate for non-repudiation, compliance audit and send and receive functions.

Kwan teaches digital certificates and the recovery of encryption keys (*abstract*). Kwan teaches including third party archiving of certificate for non-repudiation, compliance audit and send and receive functions (*abstract; paragraph [0022], [0023]*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of digital certificates and recovery of encryption

keys as taught by Kwan in the modified system of Alder, Bohrer, Cordery, and Aull in

order to provide the ability to allow the archival of the private keys corresponding to their

digital certificates to be outside of the control of the Certificate Authority in the event the

user needs for any reason the certificate to be recovered (*abstract*).

Claims 12 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Alder in view of Bohrer in view of Cordery in view of Aull in further view of

Tan.

As to claims 12 and 27, neither Alder, Bohrer, Cordery, nor Aull teach the

binding of a users identity and access authorizations to a physical device, such as a

USB key, and challenging the key at a remote email server in order to gain access to

the users authorized email box and messages.

Tan teaches another method of facilitating secure electronic communications

through a network (*abstract; column 1, line 29-42*). Tan teaches a USB key that

containing encryption and processing circuitry, authorized user bound identity

information and volatile and/or non-volatile memory that stores the algorithms used to

query for said data fields (*column 3, line 51-54; and column 3, line 62 to column 4, line

58*).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the method of facilitating electronic communications as

taught by Tan in the modified system of Alder, Bohrer, Cordery, and Aull in order to

provide secure communications by validation and authentication of external systems to

secure the privacy of electronic data exchange and transactions of the system (*column 1, line 29-42; and column 4, line 59 to column 5, line 3*).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to /MALCOLM CRIBBS/ whose telephone number is (571)270-1566. The examiner can normally be reached on 9-5 m-f.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/MALCOLM CRIBBS/
Examiner
Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432